ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

Securing Remote Medical Sensor Data by Adapting Paillier Cryptosystem Mechanism

Navya D [1], Rashmi M [2]

M.Tech Student, Department of Computer Science & Engineering, Srinivas Institute of Technology, Mangaluru, Karnataka, India[1]

Associate Professor, Department of Computer Science & Engineering, Srinivas Institute of Technology, Mangaluru, Karnataka, India[2]

ABSTRACT: In recent times, healthcare applications are widely being used for remote patient monitoring and in hospitals using wireless sensor networks. Wireless medical sensor networks are highly vulnerable to different kind of attacks such as eavesdropping, modification, data breach etc which is a potential threat to patient sensitive physiological data. Security for wireless medical sensor networks is one of the major requirements in order to attain few issues like authentication, integrity and confidentiality. A considerable measure of work has been done to secure wireless medical sensor networks. The existing healthcare solutions can protect information amid transmission but in any case fails to stop inside attack where the sensitive patient data will be revealed by the malicious database administrator. The proposed system presents a practical approach to overcome this issue by making use of multiple data servers for storing patient sensitive data. The primary contribution of this system is secure transmission of patient sensitive data to multiple data servers and performing statistical analysis on the patient data using Paillier cryptosystem by ensuring patients' privacy.

KEYWORDS: Wireless medical sensor network, patient data privacy, Paillier cryptosystem, statistical analysis.

I. INTRODUCTION

Wireless Sensor Networks are widely used in medical fields which are referred to as wireless medical sensor networks (WMSNs). The healthcare applications use medical sensors to sense the patient's physiological data and transmit them wirelessly across the public channels and store in the back-end databases. They are considered as promising fields where the patients can be monitored continuously in hospitals and also at home. The physicians can monitor their patients remotely by accessing patients' health data through wireless medical sensor networks. The medical researchers can use the healthcare application for their research purpose and perform statistical analysis on patient physiological data. The patients' data will be transmitted to data server and stored in some back-end systems. The patients' privacy becomes vulnerable if the healthcare applications are deployed without considering the security. Therefore, a paramount necessity for healthcare application is security, particularly in the account of patient's privacy. Wireless medical sensor networks conclusively improve patients' nature of care without exasperating their solace. There exist a lot of potential security threats to the patient's sensitive health data during transmission from the medical sensors to the physicians or medical researchers. Various security threats to healthcare applications [1], [2] that affect patients' data privacy are summarized as follows.

Impersonation attack is a threat to the authenticity of patient's data. In a healthcare application, an adversary might impersonate a wireless access point, while data is being sent to a remote location. As a result, this will lead to false alerts and the physicians could start an emergency rescue operation for an individual who is non-existent. This will even defeat the reason of wireless healthcare application.

Eavesdropping is a threat to the data privacy of patients when attacker performs this type of attack. An eavesdropper may be equipped with intensively powerful receiving antenna and can retrieve the sensitive patient data from medical

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

sensors and examines the patient's health information. The eavesdropper might even post the sensitive patient data on social networking sites which is a genuine risk to patient privacy.
Modification is a threat to the data integrity of patient data. The intruder can intercept the patient's sensitive health data during transmission from the public channels and perform some alterations on the data. This could be a threat to patients when this altered data is sent to the doctors for monitoring which could result in false readings. For example, if a patient's actual body temperature reading is 103^0 F and the intruder alters it to some normal temperature reading, the physician might think that the patient's health condition is normal and doesn't take any measures.
Data breach is again a threat to the data privacy of patients. Data breach attack is a situation in which confidential patient health data has possibly been seen or utilized by an adversary who is unauthorized to do so. Considering an example, a database administrator who is malicious may retrieve the patient health data like his identity and home address for his own advantage. He can claim insurance with the patient's identity and also perform other medical frauds. Sometimes this type of attack can also lead to life threatening risk. There are few more security attacks on remote medical sensor networks such as Sybil attack, grey-hole attack, denial of service attack, data spoofing etc.
In order to protect the patient's remote medical sensor data against different attacks, the existing solutions are providing encryption based approaches for data transmission. They include public key encryption or secret key encryption. In secret key based mechanisms, it is assumed that the symmetric keys are pre-deployed in servers and sensors in advance. In this type of solution, AES cryptosystem is used for encryption and Message authentication code for authentication. In public key based mechanisms, RSA or Diffie-Hellman key exchange protocol is used for generating secret keys and for encryption.
The Paillier cryptosystem is used for providing assured security for patient data during transmission. This cryptosystem has an added benefit in its homomorphic properties where by providing only a set of plaintexts and the public key parameters, the product of the plaintexts is achieved. On the decrypting side, the user can decrypt the received data and obtain the sum of the plaintexts. Paillier cryptosystem can be useful for those applications which need top of the line security and summation of the set of plaintexts.
The existing solutions can provide privacy to the patients' data by ensuring protection against outside attacks but fails to provide protection against the inside attacks. Some of the existing solutions don't provide security at all and some solutions do provide security for the data transmitted over channels. The existing solution deals with security of patient data by using three servers to store patient information [1]. They split the received data from sensors into three parts and sends to three servers using a secure channel where the secret keys are pre-deployed in sensors and servers. This solution can provide protection to the sensitive patient data as long as only one data server is compromised. If the attacker is successful in compromising two of the three data servers then the existing solution is a failure. The proposed system provides a practical approach to overcome this issue and also provides protection against inside attacks. In the proposed system, even if the attacker is successful in compromising two of the three data servers, the solution is still secure.

II. RELATED WORK

Sharemind system for providing privacy to the medical sensor networks [3], is a medical care application used or home patient monitoring and it is more secured than the other key based solution which ensure security for the sensitive data during transmission. The other existing solutions can provide security against outside attacks but this system assures security for both outside as well as inside attacks where the inside attacker is the administrator of the patient database. This approach utilizes an effective system known as Sharemind which is capable of processing the encrypted data without converting it to the decrypted format. Sharemind system comprises of three servers used for processing patient data and storing in their respective back end databases. They have a unique capability of splitting the patient's health attribute value into three random parts and send them to three servers. The secret keys are pre-deployed in bio sensors and data servers to provide a secure channel for transmission. The data servers can perform computations on the data when the doctors or medical researchers issue commands requesting to access patient data. The main limitation of this system is that it is limited to only 3 servers and is not flexible to add more number of servers for better security. This approach is secured until an attacker is successful in compromising one out of 3 data servers. If more than one server is compromised then this system is prone to leakage of data.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

CodeBlue for medical care [4], provides a hardware and software platform that can be deployed on wireless medical sensor networks. This architecture proposes a publish/subscribe architecture to provide some protocols for multihop routing and device discovery. In this system, a special device called Mote-Track is utilized to track the specific location of the patients. This system requires wearable sensor platforms which includes wearable, small and lightweight sensors. It provides reliable communication ensuring the data availability. It supports multiple receivers where the receivers include doctors, nurses or caregivers who monitor patient health information. It also supports device mobility, for example, if suppose doctors are moving from room to room for rounds, the device should be quick enough to find new routes. In this system, the medical sensors will sense the patient's body and then transmit the relevant data wirelessly to the doctor's devices such as PDA or a laptop for monitoring. The doctors issue a query using their handheld devices to receive the patients' data. Using the publish/subscribe architecture, the medical sensors can publish their sensed data into a particular channel and thereby the doctors will subscribe to that channel with laptops or any other devices to retrieve health information. The major issues with CodeBlue architecture were that, there is no security assurance for data during transmission. The authors suggested that the Elliptic curve cryptography can be used for this system to provide security for data transmission in future work. This system is vulnerable typical attacks such as denial of service attack, masquerading attack, snooping, routing loop attack etc.

Alarm-Net architecture [5], is a medical care application that mainly focuses on home patient monitoring. This architecture includes various components such as mobile body networks which comprises of wearable medical sensors worn by patients which helps in physiological sensing. The patient data is then sent over wireless network to the user and stored in back end systems. Another component is emplaced sensor networks which comprises of spatially distributed sensors to sense dust, sound etc. The alarm gate application is a gateway which provides a connection between back end systems and user interface to store received data. SeeMote is a wearable interface used in this system which provides graphical alerts to the patients. In this system, Secure Remote Password (SRP) protocol is utilized to protect the IP network. Only the authorized users can query the wireless network for the patient's physiological data. Medical sensors will respond to the user with a single record. The Alarm-Net architecture provides data confidentiality for the patients' data and authentication for the users. This system has a few limitations which show that AES encryption scheme is used to encrypt the patient data but this system does not support AES decryption during transmission. The intermediate data during transmission cannot be accessed when needed. This architecture also has a loop hole where the resident's location is leaked which is a confidentiality attack.

SNAP model for patient assessment [6], is a model for showing the security considerations in other medical care applications. In this system, Elliptic curve cryptography (ECC) mechanism, which is a public key approach, is used to ensure security of patients' data during transmission. The major drawback of this system is that it does not check for the authentication of the user requesting to access patient data. This results in unauthorized access to the sensitive patient data which poses a risk to patient privacy. The patient health data which is captured from the medical sensors is sent to the controller of the application as a plaintext. This shows that data confidentiality is not achieved in this application. The intruder may inject malicious information into the patient data during transmission and perform modification attack or replaying attack on the data. In this system, an effective group key management is presented which is proved to be computation ineffective and cannot satisfy the precise delay requirements in sensor networks. Therefore, Snap model becomes vulnerable to various kinds of attacks one of them being denial of service (DOS) attacks. As this system uses a public key cryptography approach to secure the data, the bio sensors which is said to have low computation power will not be able to successfully support high computations required for public key based methods. Hence Snap model fails to provide high end security for sensitive patient data.

Wireless Medical sensor networks secured with a lightweight encryption method [7], provides an architecture containing a large scale of wireless medical sensor networks which compromises of Patient area networks (PAN). Bio sensor nodes and a processing device called as controller such as laptop or any handheld devices are the components in Patient area networks. The medical sensors have the responsibility of assembling all the physiological data of patients and transmit them to the controller of this system. The controller is responsible to send data to the central server in a secure channel. This system enforces authentication check for the users requesting to access the patient health information. Hence, only the authorized users can take control of the patient area network and issue commands to attain the patient health information. This system does not provide direct communication between the medical sensors and the users requesting the data. The medical sensors communicate directly only with the controller of the system. The authentication of thousands of users requesting for data is computationally infeasible for the bio sensors with low

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

computation power. For a reliable secured transmission of data and data access control this system employs key updating mechanism using the hash chain approach. It also employs the proxy protected signature technique. This technique produces a special signature called as proxy protected signature by warrant to ensure authentication of the users. The drawback of this approach is that it can be used only by the physicians and not the researchers who is interested in analysis results. This system makes use of a single central server for processing the received data and storing them. If an adversary is able to compromise this server then all the sensitive data is leaked.

III. SYSTEM ARCHITECTURE

This paper proposes an approach which provides high end security for the patient's sensitive physiological data and assures maximum privacy for the patients. This approach deals with the security of data by using a cryptography mechanism called Paillier cryptosystem [8], which has a unique homomorphic property of producing the sum of plaintexts while encrypting the product of cipher texts. This mechanism is an essential approach in this proposed system. The architecture of proposed method is shown in Figure 1.

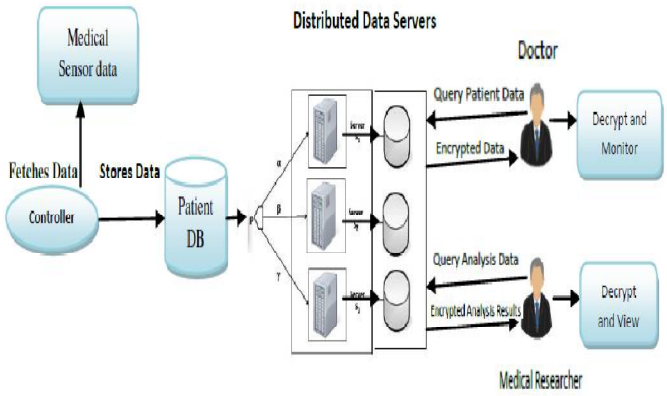

Figure 1: System Architecture

The main focus of the proposed system is securing the remote medical sensor data and performing statistical analysis on the received data. This system makes use of three data servers to process the patients' physiological data received from the bio sensors and store the data in their respective back end databases for further query processing. Like other healthcare applications, the proposed system has four components as follows.

- A wireless medical sensor network data server which stores the entire patient's health data that is received from the medical sensors and forwards the patient data to the patient's database system.
- The database system of patients which is responsible to store the patient records and provides services for doctors or medical researchers to query the patient database system.
- A data access control system for patients, which is utilized by the doctor to gain access to the patient health records and continuously monitor the patients remotely.
- A data analysis system for patients, to be used by the medical researcher to perform statistical analysis on the patients' data.

A. Data Collection protocol

This is the first deployment phase in the proposed system which is between the medical sensor data server and the three data servers which is handled by the controller. Here the three different secret keys are hardcoded into the three servers and in the controller system to transmit data securely. The controller splits the patient data (e.g., body temperature reading) into three random parts using the SplitInformation algorithm and sends to three data servers by encrypting with secret key based AES algorithm. The original value of patient data ρ is split into three parts as,

$$\rho = \alpha + \beta + \Upsilon \quad (1)$$

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

Equation (1) shows that the original value is split into three parts α, β, ϒ such that their sum equals the original value. This split part are first decrypted and stored by three data servers in their respective databases. Here, SHA-3 hashing technique [9] is used to check the authentication of the user.

B. Access Control Protocol

This phase is an initialization phase before the doctors could gain access to the patient's physiological data. In this phase, first the public and secret keys are generated for Paillier cryptosystem mechanism and Digital Signature algorithm is used for creating digital signatures [10] to verify whether the doctor has the authority to gain access to the patient data. When the doctor queries the patient data, he has to first submit his digital signature to the three data servers. The servers will verify the signatures and checks for the access control policies of the doctor. If he is authorized then [11] server SR_1 picks a random value r_1 belonging to the set of integers and encrypts the split value α using Paillier encryption and sends C_1 to data server SR_2. The data server SR_2 picks a random value r_2 belonging to the set of integers and encrypts the split value β Paillier encryption and sends the product of C_1C_2 to the data server SR_3. The data server SR_3 picks a random value r_3 belonging to the set of integers and encrypts the split value ϒ using Paillier encryption and sends the product of C1C2C3 to the doctor. The doctor can decrypt the data and obtain the value $\rho = \alpha + \beta + \Upsilon$ where ρ is the original patient health attribute value.

C. Statistical Analysis Protocol

This phase is used by the medical researchers who want to obtain the analysis results only. Various analyses are performed such as average analysis, variance analysis, correlation analysis and regression analysis. The medical researcher should first generate a digital signature and submit a query as to which analysis he wants the servers to perform. After the three data servers receives the request, they first check for the authentication of the medical researcher and his access control policies. If the researcher is authorized, the three servers cooperate to perform computations on the patient data and encrypt the data using Paillier encryption scheme as shown before and forward them to the researchers. After receiving the statistical analysis results, the researcher decrypts the data and views the analysis results.

IV. EXPERIMENTAL RESULTS

The proposed method is expected to secure the patient physiological data during transmission and this solution is secure even though two of the three data servers are compromised by the adversary. That is, as long as one of the three servers is not compromised, the proposed system assures high end security to the patients. This solution is successful in providing protection against outside attacks and also inside attacks where the malicious administrator of the database of patients may capture the patient health data and perform medical frauds for his personal advantages. Hence the proposed system accomplished to provide patient privacy using the Paillier cryptosystem mechanism. Section V presents conclusion.

V. CONCLUSION

This paper presents an efficient approach to provide high end security for wireless medical sensor data. Unlike other healthcare solutions, this system utilizes three data servers to store the split values of patient physiological data thereby providing more security to the patient data. The communication between the medical data server and the three data servers for processing is secured using the lightweight encryption method and SHA-3 based hashing technique. To preserve the privacy of the data, data collection protocol is implemented to split the patient health data into three random parts and store in three data servers. Access control protocol is used where the three data servers provide the doctor with the patient health data. Statistical analysis protocol is used where the three data servers process some queries and produce the analysis results for the medical researcher. This solution requires that at most one data server can be compromised. This solution can protect the privacy of patient data even if two data servers are compromised.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

REFERENCES

[1] P. Kumar, Y. D. Lee, H. J. Lee. "Secure Health Monitoring Using Medical Wireless Sensor Networks". In Proc. 6th International Conference on Networked Computing and Advanced Information Management, pages 491-494, Seoul, Korea, 16-18 August 2010.

[2] P. Kumar and H. J. Lee. "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey". Sensors 12: 55-91, 2012.

[3] D. Bogdanov, S. Laur, J. Willemson. "Sharemind: a Framework for Fast Privacy-Preserving Computations". In Proc. ESORICS'08, pages 192-206, 2008.

[4] D. Malan, T. F. Jones, M. Welsh, S. Moulton. "CodeBlue: An Ad-Hoc Sensor Network Infrastructure for Emergency Medical Care". In Proc. MobiSys 2004 Workshop on Applications of Mobile Embedded Systems (WAMES'04), Boston, MA, USA, 6-9 June 2004.

[5] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu,L. Fang, Z. He, S. Lin, J. Stankovic. "ALARM-NET: WirelessSensor Networks for Assisted-Living and Residential Monitoring". Technical Report CS-2006-01; Department of Computer Science, University of Virginia: Charlottesville, VA, USA, 2006.

[6] K. Malasri and L. Wang, "Addressing security in medical sensor networks," in Proc. ACM HealthNet, 2007, pp. 7–12.

[7] D. He, S. Chan and S. Tang. "A Novel and Lightweight System to Secure Wireless Medical Sensor Networks". IEEE Journal of Biomedical and Health Informatics, 18 (1): 316-326, 2014.

[8] X. Yi, J. Willemson, F. Nat-Abdesselam. "Privacy-Preserving Wireless Medical Sensor Network". In Proc. TrustCom'13, pages 118-125, 2013.

[9] SHA-3 Standard: Permutation-Based Hash & Extendable- Output Functions. Draft FIPS PUB 202, May 2014. http:csrc.nist.govpublicationsdraftsfips202fips202draft.pdf

[10] Signature Standard (DSS). FIPS PUB 186-4, July 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[11] Xun Yi, Athman Bouguettaya, Dimitrios Georgakopoulos, Andy Song and Jan Willemson. "Privacy Protection for Wireless Medical Sensor Data", IEEE Transactions on Dependable and Secure Computing, 2015.